5. NSE scripts in Nmap: where automation meets network domination!

When utilizing Nmap Scripting Engine (NSE), we harness a powerful capability within Nmap to automate and extend its network scanning functionalities.
NSE scripts enable us to perform a wide range of tasks beyond basic port scanning, including service version detection, vulnerability detection, enumeration of specific protocols like `SMB` and `DNS`, and even complex tasks like brute-force attacks and web application scanning.

Write `a bash script` that performs comprehensive network reconnaissance using Nmap with specific NSE scripts:

- Your script should accept `a host` as an arguments `$1`
- Your script should probe open ports to determine service/version information.
- Your script should enable OS detection, version detection, script scanning, and traceroute.
- Your script should **sequentially** execute multiple NSE scripts to detect vulnerabilities across various services:
  - Retrieve service banners from open ports.
  - Enumerate supported `SSL/TLS` ciphers..
  - Run default scripts `default` defined by Nmap for basic enumeration tasks.
  - Enumerate `SMB` (Server Message Block) domains.
- Save the output to `service_enumeration_results.txt` for later analysis.

Depending on the scanned network, the output could change.

```
┌──(maroua)-[~/0x07nmappostportscanscripting]
└─⚑ sudo ./5-service_enumeration.sh scanme.nmap.org
[sudo] password for maroua:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-21 11:23 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.35s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
|banner: SSH-2.0-OpenSSH6.6.1p1 Ubuntu-2ubuntu2.13
| ssh-hostkey:
```

```
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|http-server-header: Apache/2.4.7 (Ubuntu)
|http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
| banner: \x01\x01\x00\x18t@\xD9\x9BfuY?\x00\x00\x00\x00t\xDF\x0A.\xD1>\x
|AD\x82\x03M\xD28\x8D\x8C\xF0\xB3t\x1F'x4Y\x81X5\xD9\x90\x18\xA3\x16...
31337/tcp open  tcpwrapped
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X (85%)
OS CPE: cpe:/o:linux:linuxkernel:3.8 cpe:/o:linux:linuxkernel:4.4
Aggressive OS guesses: Linux 3.8 (85%), Linux 4.4 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linuxkernel



TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   1.10 ms   _gateway (192.168.1.1)
2   98.52 ms  192.168.60.1
3   98.53 ms  196.203.189.161
4   98.50 ms  193.95.96.6
5   98.54 ms  193.95.0.150
6   ...
7   99.31 ms  195.72.67.33
8   200.80 ms ae24.cr4-nyc6.ip4.gtt.net (213.200.121.6)
9   200.66 ms ip4.gtt.net (98.124.184.66)
10  200.34 ms ae2.r02.lga01.icn.netarch.akamai.com (23.203.156.40)
11  200.38 ms ae13.r01.ewr01.icn.netarch.akamai.com (23.32.63.214)
12  200.39 ms ae19.r01.ord01.icn.netarch.akamai.com (23.193.113.37)
13  303.62 ms ae16.r01.sjc01.icn.netarch.akamai.com (23.32.62.79)
14  303.60 ms ae1.r11.sjc01.ien.netarch.akamai.com (23.207.232.35)
15  303.64 ms a23-203-158-51.deploy.static.akamaitechnologies.com
(23.203.158.51)
16  ... 18
19  303.74 ms scanme.nmap.org (45.33.32.156)
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1171.07 seconds
```

The command:

```
nmap -sV -A -O --script banner,ssl-enum-ciphers,default,smb-enum-domains -oN
service_enumeration_results.txt $1
```

Explanation:

1. `nmap`:
   - Runs the Nmap network scanner.
2. `-sV`:
   - **Service Version Detection**: This flag tells Nmap to attempt to determine the version of the services running on open ports. It will probe services and report the version numbers, which can help identify vulnerabilities based on known software versions.
3. `-A`:
   - **Aggressive Scan**: This flag enables a combination of advanced scanning options, such as:
     - **Operating System Detection** (`-O`).
     - **Version Detection** (`-sV`).
     - **Script Scanning** (`--script`).
     - **Traceroute**.
   - It's a comprehensive scan that gathers as much information as possible about the target.
4. `-O`:
   - **OS Detection**: This option allows Nmap to attempt to detect the target's operating system based on TCP/IP stack fingerprinting.
5. `--script`:
   - Runs specified **NSE scripts** to gather additional information about the target's services. The scripts listed here will provide valuable insights into the target's configuration and vulnerabilities.
   - The scripts used in this command are:
     - `banner`: Retrieves and displays service banners, which typically provide information about the software and version running on the open ports (e.g., Apache version, OpenSSH version).

    - **`ssl-enum-ciphers`**: Enumerates the supported SSL/TLS ciphers of a target. This script is useful for identifying weak or deprecated ciphers that could expose the target to attacks.
    - **`default`**: Runs the default set of scripts associated with common vulnerabilities and checks.
    - **`smb-enum-domains`**: Enumerates SMB domains on the target. It is useful for identifying Windows domains, domain controllers, and other SMB-related configurations.
6. **`-oN service_enumeration_results.txt`**:
    - **Output to File**: This option directs the results to a file named **`service_enumeration_results.txt`** in **normal output format** (`-oN`). This format provides a human-readable summary of the scan results.
7. **`$1`**:
    - This is a positional parameter representing the **target IP address** or **hostname**. When the command is run, `$1` will be replaced with the actual target, like `192.168.1.10` or `example.com`.

How It Works:

- **Service Version Detection (`-sV`)**: Nmap will probe open ports to detect the service version. This helps identify potential vulnerabilities associated with specific versions of services.
- **Aggressive Scan (`-A`)**: Nmap will also try to detect the target's OS, run a set of default scripts, and perform other tests to gather extensive information.
- **Operating System Detection (`-O`)**: Nmap will attempt to guess the OS based on network behavior and other clues.
- **NSE Script Execution**:
    - **`banner`**: Will retrieve service banners from open ports, such as the HTTP version or SSH version.
    - **`ssl-enum-ciphers`**: Will provide a detailed list of supported SSL/TLS ciphers, helping to identify weak or outdated ciphers that can be exploited.
    - **`default`**: Will run a set of common vulnerability checks and other useful scripts.
    - **`smb-enum-domains`**: Will gather information about SMB shares and domains on Windows systems.
- **Results**: The scan results will be saved to `service_enumeration_results.txt` for later analysis.

Example Usage:

If you want to scan a target with IP `192.168.1.10`, the command would be:

```
nmap -sV -A -O --script banner,ssl-enum-ciphers,default,smb-enum-domains -oN service_enumeration_results.txt 192.168.1.10
```

Sample Output in `service_enumeration_results.txt`:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-28 15:30 UTC
Nmap scan report for 192.168.1.10
Host is up (0.0010s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.6p1 Debian 4 (protocol 2.0)
| banner:
|   SSH-2.0-OpenSSH_7.6p1 Debian-4
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_AES_128_CBC_SHA1
|       TLS_RSA_WITH_AES_256_CBC_SHA1
|       ...
|   TLSv1.3:
|     ciphers:
|       TLS_AES_128_GCM_SHA256
|       TLS_AES_256_GCM_SHA384
|   (some ciphers weak or deprecated)
|_  443/tcp open  https       Apache httpd 2.4.38 (Debian)
| banner:
|   HTTP/1.1 200 OK
| smb-enum-domains:
|   Enumerating SMB domains...
|   Domain: WORKGROUP
|   SMB Version: 3.0
|   Domain Controller: 192.168.1.10
|   (additional information about shares and services)
|_  (other detected SMB shares, users, etc.)

Nmap done: 1 IP address (1 host up) scanned in 15.10 seconds
```

What You Learn From This Output:

1. **SSH Version**: The target is running OpenSSH 7.6p1 Debian 4.
2. **SSL/TLS Ciphers**: The server supports multiple SSL/TLS versions and ciphers, and it may have weak or deprecated ciphers.
3. **HTTP Service**: The target has an Apache HTTP server (version 2.4.38) running on port 443, which might be vulnerable to specific issues.

4. **SMB Domains**: The target is part of the `WORKGROUP` domain and is running SMB version 3.0, which could provide further avenues for SMB-related attacks or enumeration.

Benefits:

- **Comprehensive Information**: This command will gather extensive details about the target, including service versions, SSL/TLS configurations, and SMB domain information.
- **Easy Documentation**: The output is saved to a text file, making it easier to analyze, review, and share.

Limitations:

- **Target-Specific**: The scan is designed to work with specific services and may miss vulnerabilities or misconfigurations outside of these services.
- **False Positives/Negatives**: Some services might be misidentified, or version detection might fail if the service is obfuscated or protected.

Improvement Suggestions:

- Combine with other scripts to increase coverage, such as:

```
nmap -sV -A -O --script banner,ssl-enum-ciphers,default,smb-enum-domains,http-vuln\* -oN service_enumeration_results.txt $1
```

- Use additional output formats for better automation or integration with other tools:

```
nmap -sV -A -O --script banner,ssl-enum-ciphers,default,smb-enum-domains -oX service_enumeration_results.xml $1
```

This command provides a solid baseline for service enumeration, helping you identify vulnerabilities and misconfigurations that could be leveraged in an attack.